Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Σχολή Θετικών Επιστημών

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Εργασία στο μάθημα της Κρυπτογραφίας

Φτιάκας Σωτήριος ΑΕΜ: 3076

Μπάρμπας Γρηγόριος ΑΕΜ: 3108

3 Ιουνίου 2020

Περιεχόμενα

Περίληψη

....

Θέμα 1

Θέμα 2

Θέμα 3

Vigenere

No3_Vigenere.ipynb

Θέμα 4

Θέμα 5

Dictionary Attack

No5_DictionaryAttack.ipynb

Θέμα 6

Θέμα 7

Shift Operator with XOR

m: 16-bits

$$c = m \oplus (m << 6) \oplus (m << 10)$$

Όπου $m << a$ είναι κύλιση προς τα αριστερά κατά a-bits.

Για μήνυμα m και κλειδί k ισχύει: Αν $c = m \oplus k$, τότε $m = c \oplus k$

Επιπλέον, στην αρχική μας συνάρτηση κρυπτογράφησης, μπορούμε να κυλίσουμε και τα δύο μέλη ταυτόχρονα.

$$(c << 2) = (m \oplus (m << 6) \oplus (m << 10)) << 2$$

$$\Leftrightarrow (c << 2) = (m << 2) \oplus (m << 8) \oplus (m << 12)$$

Σημείωση: το $x << i$ θα συμβολίζεται ως x_i για ευκολία.

Συνεπώς θα έχουμε:

$$c_0 = m_0 \oplus m_6 \oplus m_{10} \quad (1)$$

$$c_2 = m_2 \oplus m_8 \oplus m_{12} \Rightarrow m_8 = m_2 \oplus m_{12} \oplus c_2 \quad (4)$$

$$c_4 = m_4 \oplus m_{10} \oplus m_{14} \Rightarrow m_{10} = m_4 \oplus m_{14} \oplus c_4 \quad (2)$$

$$c_6 = m_6 \oplus m_{12} \oplus m_0 \quad (5)$$

$$c_8 = m_8 \oplus m_{14} \oplus m_2$$

$$c_{10} = m_{10} \oplus m_0 \oplus m_4$$

$$c_{12} = m_{12} \oplus m_2 \oplus m_6$$

$$c_{14} = m_{14} \oplus m_4 \oplus m_8 \Rightarrow m_{14} \oplus m_4 = m_8 \oplus c_{14} \quad (3)$$

Ξεκινώντας από την (1) έχουμε διαδοχικά:

$$c_0 = m_0 \oplus m_6 \oplus m_{10}$$
$$(2) \Rightarrow c_0 = m_0 \oplus m_6 \oplus m_4 \oplus m_{14} \oplus c_4$$
$$(3) \Rightarrow c_0 \oplus c_4 = m_0 \oplus m_6 \oplus m_8 \oplus c_{14}$$
$$(4) \Rightarrow c_0 \oplus c_4 \oplus c_{14} = m_0 \oplus m_6 \oplus m_2 \oplus m_{12} \oplus c_2$$
$$(5) \Rightarrow c_0 \oplus c_4 \oplus c_{14} \oplus c_2 = m_2 \oplus c_6$$
$$\Rightarrow c_0 \oplus c_4 \oplus c_{14} \oplus c_2 \oplus c_6 = m_2 \quad (6)$$

Κάνουμε κύλιση και στα δύο μέρη του (6) προς τα δεξιά και έχουμε:

$$m_0 = c_{14} \oplus c_2 \oplus c_{12} \oplus c_0 \oplus c_4$$

και άρα τελικά έχουμε:

$$m_0 = c_0 \oplus c_2 \oplus c_4 \oplus c_{12} \oplus c_{14}$$

Κώδικας σε python

$$No7\_Shift\_Operator.ipynb$$

Θέμα 8

Υ/X	**0**	**1**	**2**
0	1/7	1/7	1/7
1	0	1/7	1/7
2	2/7	0	0

Θέμα 9

Entropy

Αρχικά υπολογίζουμε

$$p_x(X=0)=\sum_y p_{X,Y}(0,y)=\frac{3}{7}$$

$$p_x(X=1)=\sum_y p_{X,Y}(1,y)=\frac{2}{7}$$

$$p_x(X=2)=\sum_y p_{X,Y}(2,y)=\frac{2}{7}$$

$$p_y(Y=0)=\sum_y p_{X,Y}(x,0)=\frac{3}{7}$$

$$p_y(Y=1)=\sum_y p_{X,Y}(x,1)=\frac{2}{7}$$

$$p_y(Y=2)=\sum_y p_{X,Y}(x,2)=\frac{2}{7}$$

Ισχύει ότι:

$$H(X)=-\sum_x p_X(x)\log_2 p_X(x)$$

Επομένως

$$
\begin{aligned}
H(X) &= -\frac{3}{7}\log_2\frac{3}{7} - \frac{2}{7}\log_2\frac{2}{7} - \frac{2}{7}\log_2\frac{2}{7} \\
&= -\frac{3}{7}\log_2\frac{3}{7} - \frac{4}{7}\log_2\frac{2}{7} \\
&\simeq 1.5566567074628228
\end{aligned}
$$

$$
\begin{aligned}
\Upsilon(Q) &= -\frac{3}{7}\log_2\frac{3}{7} - \frac{2}{7}\log_2\frac{2}{7} - \frac{2}{7}\log_2\frac{2}{7} \\
&= -\frac{3}{7}\log_2\frac{3}{7} - \frac{4}{7}\log_2\frac{2}{7} \\
&\simeq 1.5566567074628228
\end{aligned}
$$

Επίσης έχουμε τον εξής τύπο

$$
H(X,Y) = -\sum_x \sum_y p(x,y)\log_2 p(x,y)
$$

Άρα θα έχουμε:

$$
\begin{gathered}
H(X,\Upsilon) = -p(0,0)\log_2 p(0,0) - p(0,1)\log_2 p(0,1) - p(0,2)\log_2 p(0,2) - \\
p(1,0)\log_2 p(1,0) - p(1,1)\log_2 p(1,1) - p(1,2)\log_2 p(1,2) - \\
p(2,0)\log_2 p(2,0) - p(2,1)\log_2 p(2,1) - p(2,2)\log_2 p(2,2) \\
\simeq 2.5216406363433186
\end{gathered}
$$

Θα υπολογίσουμε την $H(Y|X)$. Χρειαζόμαστε αρχικά τα παρακάτω,

$$p_{Y|X}(y=0|x=0) = \frac{p_{X,Y}(0,0)}{p_X(0)} = \frac{\frac{1}{7}}{\frac{3}{7}} = \frac{1}{3}$$
$$p_{Y|X}(y=1|x=0) = \frac{p_{X,Y}(0,1)}{p_X(0)} = \frac{0}{\frac{3}{7}} = 0$$
$$p_{Y|X}(y=2|x=0) = \frac{p_{X,Y}(0,2)}{p_X(0)} = \frac{\frac{2}{7}}{\frac{3}{7}} = \frac{2}{3}$$
$$p_{Y|X}(y=0|x=1) = \frac{p_{X,Y}(1,0)}{p_X(1)} = \frac{\frac{1}{7}}{\frac{2}{7}} = \frac{1}{2}$$
$$p_{Y|X}(y=1|x=1) = \frac{p_{X,Y}(1,1)}{p_X(1)} = \frac{\frac{1}{7}}{\frac{2}{7}} = \frac{1}{2}$$
$$p_{Y|X}(y=2|x=1) = \frac{p_{X,Y}(1,2)}{p_X(1)} = \frac{0}{\frac{2}{7}} = 0$$
$$p_{Y|X}(y=0|x=2) = \frac{p_{X,Y}(2,0)}{p_X(2)} = \frac{\frac{1}{7}}{\frac{2}{7}} = \frac{1}{2}$$
$$p_{Y|X}(y=1|x=2) = \frac{p_{X,Y}(2,1)}{p_X(2)} = \frac{\frac{1}{7}}{\frac{2}{7}} = \frac{1}{2}$$
$$p_{Y|X}(y=2|x=2) = \frac{p_{X,Y}(2,2)}{p_X(2)} = \frac{0}{\frac{2}{7}} = 0$$

Τώρα πρέπει να υπολογίσουμε τα παρακάτω:

$$\begin{aligned}
H(Y|X=0) &= -\sum_y p_{Y|X}(y|x=0)\log_2 p_{Y|X}(y|x=0) \\
&= -(\frac{1}{3}\log_2\frac{1}{3} + 0 + \frac{2}{3}\log_2\frac{2}{3}) \\
&= -(\frac{1}{3}\log_2\frac{1}{3} + \frac{2}{3}\log_2\frac{2}{3}) \\
H(Y|X=1) &= -\sum_y p_{Y|X}(y|x=1)\log_2 p_{Y|X}(y|x=1) \\
&= -(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2} + 0) \\
&= -\log_2 2 = 1 \\
H(Y|X=2) &= -\sum_y p_{Y|X}(y|x=2)\log_2 p_{Y|X}(y|x=2) \\
&= -\log_2 2 = 1
\end{aligned}$$

Τότε θα έχουμε

$$H(Y|X) = \sum_x p_X x H(Y|X=x)$$

$$= p_X(0)H(Y|X=0) + p_X(1)H(Y|X=1) + p_x(2)H(Y|X=2)$$

$$\simeq 0.9649839288804954$$

Γνωρίζουμε επίσης ότι από το θεώρημα της αμοιβαίας πληροφορίας έχουμε

$$I(X,Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

Άρα έχουμε

$$H(X|Y) = -(H(Y) - H(Y|X) - H(X))$$
$$\simeq 0.9649839288804954$$

Τέλος,

$$\rho = 1 - \frac{H(Y|X)}{H(X)}$$
$$\simeq 0.5916727785823274$$

Κώδικας σε python

No9_Entropy.ipynb

Θέμα 10

Θέμα 11

Θέμα 12

Θέμα 13

Chinese Theorem

Έχουμε το σύστημα των γραμμικών ισοδυναμιών

$$x \equiv 9 \pmod{19}$$
$$x \equiv 9 \pmod{12}$$
$$x \equiv 13 \pmod{19}$$

Έχουμε ότι ισχύει $\gcd(12, 17, 19) = 1$, άρα δεν απαιτείται κάποια απλοποίηση.

Για την επίλυση του συστήματος χρησιμοποιούμε το Κινέζικο Θεώρημα Υπολοίπων

Έτσι έχουμε: $m = 17 * 12 * 19 = 3876$

$$M_1 = 228 y_1 \equiv 1 \mod 17 \implies 7y_1 \equiv \mod 17 \implies y_1 = 5$$
$$M_2 = 323 y_2 \equiv 1 \mod 12 \implies 11y_1 \equiv \mod 12 \implies y_1 = 11$$
$$M_3 = 204 y_3 \equiv 1 \mod 19 \implies 14y_1 \equiv \mod 19 \implies y_1 = 15$$

Τώρα πολλαπλασιάζουμε και προσθέτουμε:

$$x = 9 * 228 * 5 + 9 * 323 * 11 + 13 * 204 * 15$$
$$= 82017(1)$$

Παρατηρούμε ότι η (1) γράφεται,

$$x = 82017 = 621 + 3876k, k \in \mathbb{Z}$$

Για $k = 0$ έχουμε λύση το $x = 621$

Κώδικας σε python

$$No13\_ChineseTheorem.ipynb$$

Θέμα 14

Θέμα 15

Θέμα 16

GPG, PGP, Send Message

Μπάρμπας Γρηγόριος:

$$b641ed06419f8ff4a6447cc9fb9d2295$$

Φτιάκας Σωτήριος:

$$5f816b4f295dc95721a7a34b9fd1653a$$

Θέμα 17

Θέμα 18

secure.zip

$$9e94b15ed312fa42232fd87a55db0d39$$

Θέμα 19

Θέμα 20

Θέμα 21

Θέμα 22

3.1

Αρχικά θέλουμε να αποδείξουμε ότι οι αριθμοί της μορφής $4n+3$ δεν είναι τέλεια τετράγωνα. Αρχικά για $n \leq 0$ εύκολα παρατηρούμε ότι ισχύει η παραπάνω πρόταση. Αυτό συμβαίνει καθώς για $n = 0$ έχουμε το 3 το οποίο δεν είναι τέλειο τετράγωνο και για $n < 0$ το $4n + 3$ είναι αρνητικός.

Έστω ότι,

$$4n + 3 = a^2, \quad n, a \in \mathbb{N}^*(1)$$

Εφόσον $a \in \mathbb{N}^*$, τότε μπορούμε να πούμε ότι $a = 2k + 1, \quad k \in \mathbb{N}$.

Αντικαθιστώντας το a στην (1) έχουμε:

$$\begin{aligned} 4n + 3 = (2k + 1)^2 \implies 4n + 3 &= 4k^2 + 4k + 1 \\ &\equiv 4k^2 + 4k - 4n = 2 \\ &\equiv 2(k^2 + k - n) = 1 \\ &\equiv k^2 + k - n = \frac{1}{2} \end{aligned}$$

Το οποίο είναι άτοπο καθώς $k, n \in \mathbb{N}^*$ και άρα το $k^2 \in \mathbb{N}^*$ αλλά και όλη η παράσταση $k^2 + k - n \in \mathbb{N}$, εφόσον είναι άθροισμα των φυσικών αριθμών k^2, k και $-n$.

Συνεπώς και η αρχική ισοδύναμη υπόθεση είναι άτοπη, οπότε το $4n+3$ δεν είναι τέλειο τετράγωνο.

Για το δεύτερο ερώτημα παρατηρούμε ότι όλοι αριθμοί

$$11, 111, \ldots, 111\cdots 111, \ldots$$

μπορούν να γραφούν στην μορφής $(4n+3)+10^q$, συνεπώς αυτό το σύνολο αριθμών δεν θα έχει τέλειο τετράγωνο.

Θέμα 23

3.4

Υπάρχουν δύο περιπτώσεις που θα χρειαστεί να εξετάσουμε.

Περίπτωση 1: Για περιττό αριθμό διαδοχικών αριθμών, αυτοί οι αριθμοί θα έχουν ως μέσο έναν ακέραιο (μεσσαίος αριθμός), οπότε το άθροισμα γράφεται ως εξής:

$$sum = average * number\_of\_consecutive\_numbers$$

$$\implies sum = integer * odd\_number$$

Αυτό σημαίνει ότι το άθροισμα (sum) διαιρείται από έναν περιττό αριθμό. Αυτό όμως δεν μπορεί να είναι το σενάριο για το 2^m.

Περίπτωση 2: Ένας ζυγός αριθμός διαδοχικών αριθμών έχουν ως μέσο το μέσο του αθροίσματος των δύο μεσαίων. Συνεπώς έχουμε:

$$sum = ((sum\_of\_two\_middle\_numbers) * \frac{1}{2}) * number\_of\_consecutive\_numbers$$

$$\implies sum = (sum\_of\_two\_middle\_numbers) * \frac{1}{2} * even\_number$$

$$\implies sum = (sum\_of\_two\_middle\_numbers) * integer$$

$$\implies sum = ((k) + (k+1)) * integer \quad , k \in \mathbb{Z}$$

$$\implies sum = (2k+1) * integer$$

Το $2k+1$ είναι περιττός αριθμός, άρα το άθροισμα (sum) έχει ως παράγοντα περιττό, άρα όπως και προηγουμένως απορρίπτεται το σενάριο 2^m.

Θέμα 24

Θέμα 25

Θέμα 26

Θέμα 27

3.26

(i) Έστω ότι $d_1 = \gcd(c, b)$ και $d_2 = \gcd(ac, b)$

Τότε έχουμε $c \cdot x_1 + b \cdot y_1 = d_1$, $a \cdot c \cdot x_2 + b \cdot y_2 = d_2$ και $a \cdot x + b \cdot y = 1$, από Bezout. Αρχικά πολλαπλασιάζουμε την $a \cdot x + b \cdot y = 1$ με το d_1 και έχουμε:

$$d_1 \cdot (a \cdot x + b \cdot y) = 1 \cdot d_1$$
$$\implies a \cdot x(c \cdot x_1 + b \cdot y_1) + b \cdot d_1 \cdot y = d_1$$
$$\implies a \cdot c \cdot (x \cdot x_1) + b \cdot (a \cdot x \cdot y_1 + d_1 \cdot y) = d_1$$

Εφόσον ισχύει ότι $d_2 = \gcd(ac, b)$, τότε διαιρεί κάθε ακέραιο γραμμικό συνδυασμό των ac και b και άρα έχουμε $d_2 | d_1 \quad (1)$.

Στην συνέχεια θα πολλαπλασιάσουμε ομοίως το $a \cdot x + b \cdot y = 1$ με το d_2 και έχουμε:

$$d_2 \cdot (a \cdot x + b \cdot y) = 1 \cdot d_2$$
$$\implies a \cdot x(a \cdot c \cdot x_2 + b \cdot y_2) + b \cdot d_2 \cdot y = d_2$$
$$\implies c \cdot (a^2 \cdot x \cdot x_2) + b \cdot (a \cdot x \cdot y_2 + d_2 \cdot y) = d_2$$

Ομοίως με προηγουμένως ισχύει ότι $d_1 = \gcd(c, b)$, τότε διαιρεί κάθε ακέραιο γραμμικό συνδυασμό των ac και b και άρα έχουμε $d_1 | d_2 \quad (2)$. Από (1) και (2) έχουμε ότι $d_1 = d_2$, μη αρνητικά.

Αφού

$$(1) \implies |d_1| \leqslant |d_2|$$

$$(2) \implies |d_2| \leqslant |d_1|$$

(ii) Έστω d κοινός διαρέτης των $a + b$ και $a - b$, τότε ο d διαιρεί και το άθροισμα και την διαφορά τους.

$$d|(a + b)$$

$$d|(a - b)$$

$$d|(a + b) + (a + b) = 2 \cdot a$$

$$d|(a + b) - (a - b) = 2 \cdot b$$

Τότε έχουμε ότι:

$$d| \gcd(2a, 2b) = 2 \gcd(a, b)$$

Όμως από αρχικά δεδομένα έχουμε ότι $\gcd(a, b) = 1$ άρα τότε ισχύει:

$$d|2$$

Συνεπώς το $d \in \{1, 2\}$

Εαν a,b περιττοί τότε έχουμε το εξής:

$$a = 2k_1 + 1 \quad k_1 \in \mathbb{Z}$$

$$b = 2k_2 + 1 \quad k_2 \in \mathbb{Z}$$

Άρα θα ισχύει και το εξής:

$$a + b = 2k_1 + 1 + 2k_2 + 1 = 2k_1 + 2k_2 + 2 = 2 \cdot (k_1 + k_2 + 1) \quad (even)$$

$$a - b = 2k_1 + 1 - 2k_2 + 1 = 2k_1 - 2k_2 = 2 \cdot (k_1 - k_2) \quad (even)$$

Εφόσον και τα δύο είναι ζυγοί αριθμοί τότε οι διαιρέτες τους θα είναι ζυγοί. Όπως αποδείξαμε προηγούμενος όμως, αν d διαιρέτης, τότε $d \in \{1, 2\}$ Συμπερασματικά έχουμε ότι $d = 2$.

(iii) Έστω $d = \gcd(a, b)$ τότε $d = a \cdot x + b \cdot y, \quad x, y \in \mathbb{Z}$ Αν $i = \gcd(2^a - 1, 2^b - 1)$ τότε

$$2^a \equiv 1 \mod i$$

$$2^b \equiv 1 \mod i$$

Συνεπώς έχουμε

$$2^d = 2^{a \cdot x + b \cdot y} = (2^a)^x \cdot (2^b)^y \equiv 1 \mod i$$

Οπότε $p|2^d - 1$. Από την άλλη μεριά αν $d|a$, τότε $2^d - 1|2^q - 1$, οπότε το $2^d - 1$ αποτελεί κοινό παράγοντα. Έτσι αποδείξαμε ότι

$$\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$$

Όμως από αρχικά δεδομένα $d = 1$, άρα και η προηγούμενη σχέση γράφεται:

$$\gcd(2^a - 1, 2^b - 1) = 1$$

(iv) Παρατηρούμε ότι αν αντικαταστήσουμε τα M_p, M_q έχουμε την παραπάνω σχέση.

Θέμα 28

Θέμα 29

Θέμα 30

3.70

Υπόθεση:

$N > 2$

$N = p_1 p_2 \dots p_k$

$p_j - 1 | N - 1 \forall j$

Απόδειξη:

Έστω $\gcd(a, N) = 1$.

Από το θεώρημα του Fermat, $\forall j$, έχουμε $a^{p_j} \equiv 1 \mod p_j$.

Εφόσον $p_j - 1 | N - 1$,και άρα $a^{N-1} \equiv 1 \mod p_j$.

Δηλαδή το $a^{N-1} - 1$ είναι πολλαπλάσιο κάθε p_j.

Συνεπώς $a^{N-1} \equiv 1 \mod N$.

Θέμα 31

3.74

Παρατηρούμε ότι $561 (= 3 \cdot 11 \cdot 17)$ είναι αριθμός Carmichael. Θα βρούμε όλους του αριθμούς Carmichael μέχρι $N (= 3000)$.

Πρόταση 1: Έστω $n = p \cdot u$ όπου p είναι πρώτος. Τότε αν και μόνο αν $p - 1 | u - 1$ θα ισχύει και $p - 1 | n - 1$.

$$(n - 1) - (u - 1) = n - u = p \cdot u - u = (p - 1) \cdot u$$

Πρόταση 2: Έστω ένας αριθμός Carmichael έχει τουλάχιστον τρεις πρώτους παράγοντες. Για την απόδειξη αυτής της πρότασης εφαρμόζουμε την εξής λογική:

Έστω ότι ο n έχει δύο πρώτους παράγοντες $n = p \cdot q$ όπου p, q πρώτοι και $p > q$. Τότε $p - 1 > q - 1$, άρα το $p - 1$ δεν διαιρεί το $q - 1$. Από την πρόταση (1) το $p - 1$ δεν διαιρεί το $n - 1$. Συνεπώς το n δεν είναι αριθμός Carmichael.

Πρόταση 3: Ας υποθέσουμε ότι ο n είναι Carmicael και ότι το p και το q είναι πρώτοι παράγοντες του n. Τότε $q \not\equiv 1 \mod p$.

Έστω ότι το $q \equiv 1 \mod p$, έτσι ισχύει ότι $p | q - 1$. Τότε $q - 1 | n - 1$ καθώς θα ισχύει και ότι $p | n - 1$. Όμως αυτό είναι άτοπο καθώς ισχύει ότι $p | n$.

Εύρεση αριθμών Carmichael: Έστω αριθμός n με τρεις πρώτους παράγοντες $n = p \cdot q \cdot r$, με $p < q < r$. Από τα προηγούμενα καταλαβαίνουμε ότι χρειαζόμαστε τριπλέτες (p, q, r) για τις οποίες θα ισχύουν τα εξής:

$$(i) \quad p - 1 | q \cdot r - 1 \quad (or \quad q \cdot r \equiv 1 \mod (p - 1))$$
$$(ii) \quad q - 1 | p \cdot r - 1$$
$$(iii) \quad r - 1 | p \cdot q - 1$$

Δοθεί ένα ζευγάρι πρώτον αριθμών (p, q) με $p < q$, η ακόλουθη διαδικασία θα εντωπίσει όλους τους πρώτους $r > q$ τέτοιοι ώστε το $p \cdot q \cdot r$ να είναι αριθμός Carmichael.

Έστω οι ζυγοί διαρέτες (αν υπάρχουν) d του $p \cdot q - 1$ με $p < d < p \cdot q - 1$ και ελέγχουμε αν $d + 1 (= r)$ είναι πρώτος, εξαιρούμε το $d = p \cdot q - 1$ καθώς θα μας έδινε $r = p \cdot q$. Τότε έχουμε εξασφαλίσει το (iii) και ελέγχουμε λοιπόν αν ισχύουν τα (ii) και (ii).

Το κάνουμε για όλα τα ζευγάρια πρώτων (p, q), όπου $p \cdot q \cdot r < 3000$, για πρώτους $r > q$. Όμως λόγω του (3) αφήνουμε εκτός τους συνδυασμούς για τους οποίους ισχύει: $q \equiv 1 \mod p$ (π.χ $(3, 7)$).

Καταγράφουμε μόνο τις τιμές του d όπου το r είναι πρώτος. Όπως παρατηρούμε και στον πίνακα από κάτω δεν υπάρχει μικρότερος Carmichael με τρείς παράγοντες από τον 561.

(p, q)	$p \cdot q - 1$	d	r	(i)	(ii)	Carmichael
$(3, 5)$	14	–	–			
$(3, 11)$	32	16	17	yes	yes	$3 \cdot 11 \cdot 17 = 561$
$(3, 17)$	50	–	–			
$(3, 23)$	68	–	–			
$(5, 7)$	34	–	–			
$(5, 13)$	64	16	17	yes	yes	$5 \cdot 13 \cdot 17 = 1105$
$(5, 17)$	84	28	29	yes	yes	$5 \cdot 17 \cdot 29 = 2465$
		42	43	no		
$(5, 19)$	94	–	–			
$(7, 11)$	76	–	–			
$(7, 13)$	90	18	19	yes	yes	$7 \cdot 13 \cdot 19 = 1729$
		30	31	yes	yes	$7 \cdot 13 \cdot 31 = 2821$
$(7, 17)$	118	–	–			
$(11, 13)$	142	–	–			

Το δεύτερο ερώτημα επιλύθηκε με βοήθεια κώδικα.

Κώδικας σε python

No31_Smaller_Carmichael_4_Factors.ipynb

Αναφορές